# Chapter 1.
# General Provisions And Requirements

## Section 1. Introduction

**1-100. Purpose. This** Manual is issued in accordance with the National Industrial Security program (NISP). The Manual prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. The Manual also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.

**1-101. Authority.**

a. The NISP was established by Executive Order 12829,6 January 1993, "National Industrial Security Program" for the protection of information classified pursuant to Executive Order 12356, April 2, 1982, "National Security Information," or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated Executive Agent for the NISP by the President. The Director, Information Security Oversight Office (1S00) is responsible for implementing and monitoring the MSP and for issuing implementing directives that shall be binding on agencies.

b. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission and the Director of Central Intelligence is responsible for issuance and maintenance of this Manual. The Secretary of Energy and prescribe that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information. The Director of Central Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of Central Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information. The Secretary of Energy and the Nuclear Regulatory Commission retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954, as amended. The Secretary or the Commission may inspect and monitor contractor, licensee, grantee, and certificate holder programs and facilities that involve access to such information.

c. The Secretary of Defense serves as Executive Agent for inspecting and monitoring contractors, licensees, grantees, and certificate holders who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, certificate holders, and grantees and their respective employees. The Heads of agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on their behalf.

d. The Director, 1S00, will consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the NISP.

e. Nothing in this Manual shall be construed to supersede the authority of the Secretary of Energy or the Chairman of the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; or detract from the authority of installation Commanders under the Internal Security Act of 1950; the authority of the Director of Central Intelligence under the National Security Act of 1947, as

**1-102. scope.**

a. The NISP applies to all executive branch departments and agencies and to all cleared contractor facilities located within the United States, its Trust Territories and Possessions.

b. This Manual applies to and shall be used by contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination. This Manual also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to contractors that requires protection in the interest of national security. The Manual implements applicable Federal Statutes, Executive orders, National Directives, international treaties, and certain government-to-government agreements.

c. If a contractor determines that implementation of any provision of this Manual is more costly than provisions imposed under previous U.S. Government policies, standards or requirements, the contractor shall notify the Cognizant Security Agency (CSA). The notification shall indicate the prior policy, standard or requirement and explain how the NISPOM requirement is more costly to implement. Contractors shall, however, implement any such provision within three years from the date of this Manual, unless a written exception is granted by the CSA. When implementation is determined to be cost neutral, or where cost savings or cost avoidance can be achieved, implementation by contractors shall be effected no later than 6 months from the date of this Manual.

d. This Manual does not contain protection requirements for Special Nuclear Material.

**1-103. Agency Agreements.**

a. E.O. 12829 requires the heads of agencies to enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads.

b. The Secretary of Defense has entered into agreements with the departments and agencies listed below for the purpose of rendering industrial security services. This delegation of authority is contained in an exchange of letters between the Secretary of Defense and: (1) The Administrator, National Aeronautics and Space Administration (NASA); (2) The Secretary of Commerce; (3) The Administrator, General Services Administration (GSA); (4) The Secretary of State; (5) The Administrator, Small Business Administration (SBA); (6) The Director, National Science Foundation (NSF); (7) The Secretary of the Treasury; (8) The Secretary of Transportation; (9) The Secretary of the Interior; (10) The Secretary of Agriculture;(11) The Director, United States Information Agency (USIA); (12) The Secretary of Labor; (13) The Administrator, Environmental Protection Agency (EPA); (14) The Attorney General, Department of Justice; (15) The Director, U.S. Arms Control and Disarmament Agency (ACDA); (16) The Director, Federal Emergency Management Agency (FEMA); (17) The Chairman, Board of Governors, Federal Reserve System (FRS); (18) The Comptroller General of the United States, General Accounting Office (GAO); (19) The Director of Administrative Services, United States Trade Representative (USTR); and (20) The Director of Administration, United States International Trade Commission (USITC). NOTE: Appropriate interagency agreements have not yet been effected with the Department of Defense by the Department of Energy, the Nuclear Regulatory Commission and the Central Intelligence Agency.

**1-104. Security Cognizance.**

a. Consistent with 1-101e, above, security cognizance remains with each federal department or agency unless lawfully delegated. The term "Cognizant Security Agency" (CSA) denotes the Department of Defense (DoD), the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency. The Secretary of Defense, the Secretary of Energy, the Director of Central Intelligence and the Chairman, Nuclear Regulatory Commission may delegate any aspect of security administration regarding classified activities and contracts under their purview within the CSA or to another CSA. Responsibility for security administration may be further delegated by a CSA to one or more "Cognizant Security Offices (CSO)." It is the obligation of each CSA to inform industry of the applicable CSO.

b. The designation of a CSO does not relieve any Government Contracting Activity (GCA) of the responsibility to protect and safeguard the classified

information necessary for its classified contracts, or from visiting the contractor to review the security aspects of such contracts.

c. Nothing in this Manual affects the authority of the Head of an Agency to limit, deny, or revoke access to classified information under its statutory, regulatory, or contract jurisdiction if that Agency Head determines that the security of the nation so requires. The term "agency head" has the meaning provided in 5 U.S.C. 552(i).

**1-10S. Composition of Manual. This** Manual is comprised of a "baseline" portion (Chapters 1 through 11). That portion of the Manual that prescribes requirements, restrictions, and safeguards that exceed the baseline standards, such as those necessary to protect special classes of information, are included in the NISPOM Supplement (NISPOMSUP). Until officially revised or canceled, the existing COMSEC, Carrier, and Marking Supplements to the former "Industrial Security Manual for Safeguarding Classified Information" will continue to be applicable to DoD-cleared facilities only.

**1-106. Manual Interpretations.** All contractor requests for interpretations of this Manual shall be forwarded to the Cognizant Security Agency (CSA) through its designated Cognizant Security Office (CSO). Requests for interpretation by contractors located on any U.S. Government installation shall be forwarded to the CSA through the Commander or Head of the host installation. Requests for interpretation of DCIDs referenced in the NISPOM Supplement shall be forwarded to the DCI through approved channels.

**1-107. Waivers and Exceptions to this Manual.**

Requests shall be submitted by industry through government channels approved by the CSA. When submitting a request for waiver, the contractor shall specify, in writing, the reasons why it is impractical or unreasonable to " comply with the requirement. Waivers and exceptions will not be granted to impose more stringent protection requirements than this Manual provides for CONFIDENTIAL, SECRET, or TOP SECRET information.